PRIVACY BY REDESIGN: ALLEVIATING PRIVACY CONCERNS FOR THIRD-PARTY APPLICATIONS

Research-in-Progress

Heng Xu
Pennsylvania State University
University Park, USA
hxu@ist.psu.edu

Na Wang
Pennsylvania State University
University Park, USA
nzw109@ist.psu.edu

Jens Grossklags
Pennsylvania State University
University Park, USA
jensg@ist.psu.edu

Abstract

In online social networks, the aggressive way of data access and transmission by third-party applications (apps) has made privacy concerns particularly salient. Users' private information can be easily revealed by their and even their friends' use of apps. A heightened need for empowering user control for third-party apps arises due to the inability to monitor the data use by app providers within and outside of the social networking platform and the inherent uncertainty about their privacy practices. Drawing on the theoretical framework developed by Malhotra et al. (2004), we propose two improved designs of privacy authorization dialogues to encompass control and awareness as the essential factors to address users' privacy concerns toward third-party apps on Facebook. The approach of Privacy by ReDesign is employed to investigate whether users can more adequately represent their preferences for sharing and releasing personal information with these two improved designs.

Keywords: Privacy by ReDesign, information privacy, third-party applications (apps), Facebook

Introduction

The extensive disclosure of personal information by users of online social networks has made privacy concerns particularly salient. A number of studies have been conducted to investigate users' privacy attitudes (Hoadley et al. 2010; Jagatic et al. 2007) and the possible risks that users face when they fail to adequately protect their information (Gross and Acquisti 2005). An additional dimension that represents the complexity of studying privacy in the context of online social networks is added by the large amount of data collection and transmission by third-party applications ("apps"). According to a study conducted by The Wall Street Journal, many popular Facebook apps have been transmitting users' personal information and their friends' information to various advertising and data tracking firms (Steel and Fowler 2010). This particularly aggressive way of data access and transmission raises a new set of privacy challenges, because users' private information can be easily revealed by their and even their friends' use of apps. Even if some users think they set their profiles to the strictest privacy settings on Facebook, their profile information and shared contents (e.g., photos, videos, comments, and everything they shared) could be accessed or transmitted by apps due to their friends' ignorance of privacy and security (Wang et al. 2011). A heightened need for empowering user privacy control for third-party apps arises due to the inability to monitor the data use of app providers within and outside of the Facebook platform and the inherent uncertainty about their data practices.

In this research, we aim to protect users' information privacy associated with their use of third-party apps on a specific social networking platform, namely, Facebook. We integrate the theoretical framework developed by Malhotra et al. (2004) into design paths intended to produce two improved designs of privacy authorization dialogues that are specific to Facebook. Our new designs encompass *control* and *awareness* as the essential dimensions of users' privacy concerns in the context of third-party apps on Facebook. Through a field experiment designed to study users' real behaviours, we aim to examine the extent to which users can more adequately represent their preferences for sharing and releasing personal information by using our new interface designs of privacy authorization dialogues.

Conceptual Foundation

Privacy by ReDesign

With this work, we aim to provide a succinct example of *Privacy by ReDesign*. According to Cavoukian and Prosch (2011), "[t]he reality … is that it is not always possible to embed privacy directly from the outset. Most organizations operate in the context of existing, relatively mature IT systems and businesses practices, which they have developed and evolved over time, as business or other needs have dictated." System improvements are incremental, seldom revolutionary. As a result, the integration of privacy enhancing features into existing systems often happened using an ad hoc approach. In this work, we believe that the notion of *Privacy by ReDesign* can be well applied to the platform of Facebook, as it constantly changes its specific features and interface details while aiming for a consistent and recognizable overall user experience. As a result of the goal of rapid network growth, a careful design of appropriate privacy features from the outset was likely not always prioritized. However, as a more mature platform, pressure from users and regulators or novel business needs (e.g., in the case of third-party apps) lead to a re-examination and successive iterative improvements of existing privacy enhancing features.

This notion of *Privacy by ReDesign* is in line with the paradigm of design science in the Information Systems discipline which suggests that an improved understanding and subsequent redesigns of IT artifacts are needed in relation to their actual use, context and evolution (Gregor and Jones 2007). In re-designing the privacy authorization dialogues for third-party apps on Facebook, we have followed Hevner et al. (2004)'s design science principles which include: 1) Design as an Artifact (our two new interface designs), 2) Problem Relevance (the importance of protecting users' information privacy in their daily use of apps), 3) Design Evaluation (our ongoing evaluation of the design artifact by real users), 4) Research Contributions (the principles underlying the form of the design, as well as the act of implementing the design in the real world), 5) Design Based in a Search Process and Rigorous Research (a review of relevant literature, the use of Malhotra et al. (2004)'s theoretical framework in establishing design requirements, and our ongoing technical evaluation among real users), and 6) Communication of Research (implementation and deployment of our new interfaces in user communities and at technology policy events, and description of our design work in this paper).

Triggers of Users' Privacy Concerns

In the privacy literature, a number of conceptual papers have highlighted the difficulty in defining a common understanding of privacy (e.g., Solove 2006). Based on an interdisciplinary review of privacy literature, Smith et al. (2011) identified four definitional approaches of information privacy: privacy as a human right, privacy as a commodity, privacy as a state of limited access, and privacy as the ability to control information about oneself. To further understand how to protect information privacy through a design lens, it is also useful to relate to the triggers of users' privacy concerns. Smith et al. (1996) identified four dimensions of individuals' concerns about organizational information practices including inappropriate collection of personal information, errors in personal information, unauthorized secondary use of information, and improper access to information.

Even though privacy concerns exist in both online and offline environments, Smith et al. (1996)'s four dimensions primarily focus on individuals' concerns in the context of offline and direct marketing. Hence, Stewart and Segars (2002) suggest that Smith et al. (1996) "needs to be reinvestigated in light of emerging technology, practice and research" (p.37). To address privacy issues in the online environment, Malhotra et al. (2004) built upon Smith et al. (1996)'s four-dimension framework and proposed Internet Users Information Privacy Concerns (IUIPC) which encompasses three essential dimensions of privacy

concerns: inappropriate *collection* of personal information, lack of *control* over personal information, and lack of *awareness* of organizational privacy practices.

In this research, we ground our work in the theoretical framework of IUIPC and attempt to map these three dimensions of users' privacy concerns to the design of privacy authorization dialogues for third-party apps on Facebook. Specifically, the original design of the privacy authorization dialogue employed by Facebook (see Figure 1) has addressed the *collection* dimension of IUIPC by providing a basic notification that users' personal data are being collected. However, prior research has pointed out that such an interface to notify users about the app's information practices is uninformative and ineffective. Besmer and Lipford (2010) suggest that Facebook users are not truly understanding and consenting to the risks of apps that maliciously harvest their profile information. To address these limitations, we argue that an effective design of a privacy authorization dialogue should further address the *control* and *awareness* dimensions of IUIPC by providing: (i) options for users to control the specific types of information being accessed or used, and (ii) alert signals for users when their sensitive private information is being requested by the apps.

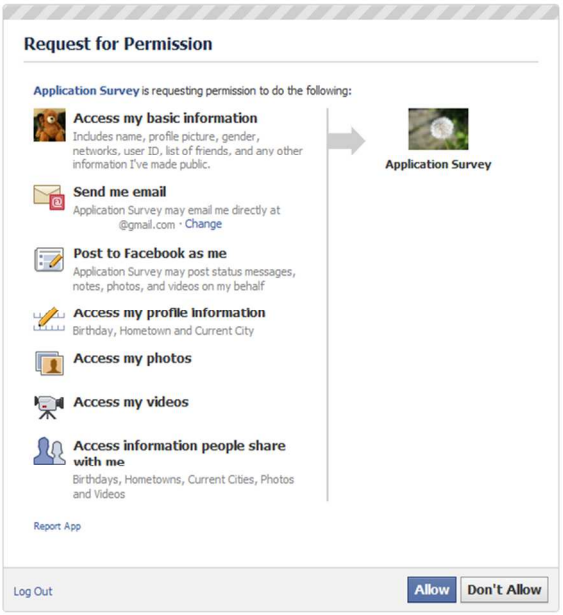

Figure 1. Original Design of the Privacy Authorization Dialogue on Facebook

Design Principles

As discussed earlier, users' privacy concerns pertaining to third-party apps serve as inspiration for our research efforts on redesigning the interface of privacy authorization dialogues on Facebook. To accomplish our goals of *Privacy by ReDesign*, we first follow Sein et al. (2011)'s design guideline to inscribe theoretical elements in the ensemble artifact (i.e., new interface of privacy authorization dialogues). In this section, we describe the starting point of our design paths by providing a conceptual mapping between three dimensions of IUIPC and our design principles.

Notifying about Data Collection: Reflecting on the origin of privacy concerns, *collection* refers to individuals' concerns about the approach and the amount of personal information demanded by others (Malhotra et al. 2004). The act of data collection forms the "foundation" of privacy concerns and predicates on the principle of equity which relates to one's gains from information exchange. Increasingly, data collection activities induce the perception of intensive data logging, as well as the impression that organizations are getting more intrusive (Sheehan and Hoy 2000). In the context of third-party apps on Facebook, the development of an app typically involves the creation of a basic authentication dialogue to notify users about apps' data collection practices (see Figure 1).

Empowering User Control: Constituting the "active" component of privacy concerns, *control* refers to the degree individuals perceive themselves to be vested with power over the procedures (Malhotra et al. 2004). While Smith et al. (1996) hint at the importance of control through their emphasis on improper access to information and unauthorized secondary use, IUIPC singles out control as one of its three essential factors. Evidence suggests that issues with access and usage are more appropriately managed through "control over who has access to personal data, [and] how personal data are used" (Phelps et al. 2000, p.29). In the original design of privacy authentication dialogues on Facebook, users do not have any control to limit the app's access to their information or restrict app's use of their information during the process of adding an app to users' profiles (Wang et al. 2011). Only after they add the app, users could potentially edit selected categories of information access or use if they found the relevant options deeply buried in their global privacy settings (Wang et al. 2011). To address this limitation, we propose:

> *Design Principle #1: The privacy authentication dialogue should provide options for a user to control an app's information access and use before adding the app to the user's Facebook profile.*

Promoting Privacy Awareness: Constituting the "passive" component of privacy concerns, *awareness* is related to an individual's knowledge of the relevant privacy context such as organizational privacy practices for online commercial transactions. Awareness provides individuals with justifications for how information is exchanged and explanations for why certain information is requested (Colquitt et al. 2001). If individuals are deprived of these contextual information, privacy concerns would prevail (Hoffman et al. 1999). Malhotra et al. (2004) thus suggest that awareness can be manifested as informational justice which emphasizes on the articulation of information. In the context of Facebook, users may easily give out their sensitive private information to third-parties, with which users' crucial identity information can be predicted. For example, information about an individual's date and place of birth can be exploited to predict his or her Social Security number (Acquisti and Gross 2009). In the original design of privacy authentication dialogues on Facebook, there is no warning mechanism to alert users when their sensitive private information is being requested by the apps. To address this limitation, we propose:

> *Design Principle #2: The privacy authentication dialogue should provide alert signals for a user when an app asks for the user's sensitive private information such as date of birth and address.*

Design and Implementation

This section discusses how the above conceptual investigations can now be employed to help structure the first iteration of our design. Below we discuss our design solutions in detail.

Empowering Control

In the original design of the privacy authorization dialogue shown in Figure 1, many of the data request permissions are not clear to users. For example, the fourth category of data permissions in Figure 1 – "access my profile information" is requesting access to three different types of information together, including birthday, hometown and current city. This is a problematic design because a user may have different preferences for disclosing these different types of data. Further, the original design shown in Figure 1 did not differentiate the purposes of data permissions. For instance, allowing an app to collect a user's email address (i.e., data reading) and allowing an app to directly email the user (i.e., data writing) are two different types of permissions. When an app is asking for both types of permissions (data reading and writing) at the same time, users may not be able to distinguish these permissions and do not know how the app will actually handle their information.

To address these limitations, app providers should explicitly provide users with different options for disclosing different types of information, as well as clearly differentiate the purposes of data permissions. Below we describe how we approach the first design principle (shown in Figure 2).

- **The Layout of Individualized Permissions**: All types of data (basic information and extended data permissions) required by an app are listed in the first column. The first row displays the purposes of information use (including data writing and data reading). Our design decision to employ this layout of individualized permissions is consistent with many other studies that have proposed ways to improve on text-heavy privacy policies (e.g., KCG 2006; Kelley et al. 2009). The core solution from this stream of literature is to use tables or grids to distill various choices into more readable and user-friendly formats.
- **The Tick Mark and Checkbox**: Un-clickable tick marks represent those types of information that will be accessed by the app. This category of data access is non-negotiable (e.g., because of functional requirements). The checked checkbox means that users will allow the app to access and use certain information. When un-checked, users will prevent the app from accessing or using the corresponding information. In the privacy literature, instead of using the tick mark and checkbox, an alternative solution using the *Yes/No* dichotomy has been suggested by the Kleimann Group in the context of improving privacy notice in the financial sector (KCG 2006). However, we argue that the *Yes/No* dichotomy works well when there are limited columns and rows of information categories. In our representative example, we would have needed 4 columns and 11 rows of *Yes* and *No* choices, which would have been visually very difficult to parse.

Promoting Awareness

We consider the second design principle of promoting awareness to be supplementary to the first principle of empowering control in that it helps users to make meaningful choices over the now individualized control elements. As a result, we redesign the authentication dialogue to combine the elements of empowered control and increased awareness (shown in Figure 3). We expect such merged design to effectively address the complexity of the privacy decision-making problem.

- **The "i" Mark and Color Scheme**: The blue "i" mark reminds users that the basic information bundle is requested by the app and users cannot opt out from this part of the information request. The red "i" mark alerts users that certain private information is particularly sensitive, and is typically not shared with others. Both blue and red "i" marks have tooltip information provided to the user when they mouse-over the sign. In this study, our design decision on the red "i" mark was based on Acquisti and Gross (2009)'s finding that information about a user's place and date of birth can be exploited to predict the user's Social Security number. Our design decision to use colors in the design of the "i" marks is consistent with prior research indicating that the use of color could potentially improve user enjoyment when parsing the symbols (Kelly et al. 2009; Wang et al. 2011).

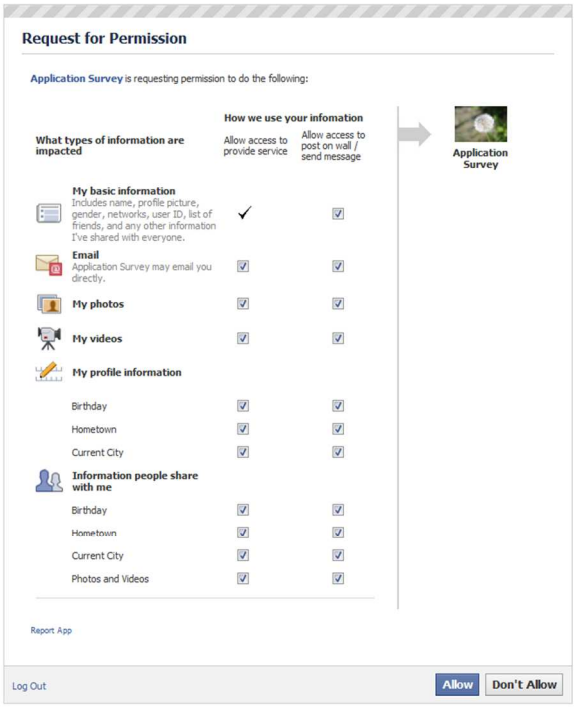

Figure 2. Proposed Design for Empowering Control

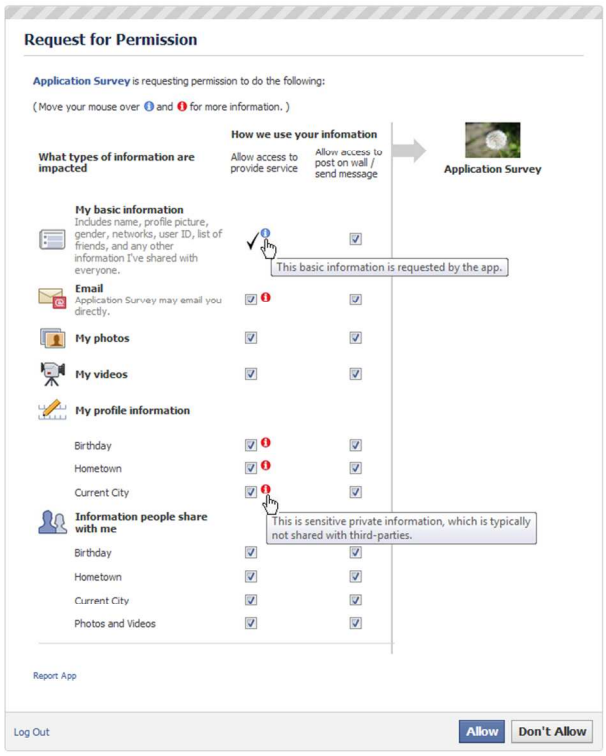

Figure 3. Proposed Design for Promoting Awareness

Technical Implementation

We have already implemented functional interfaces and tested them thoroughly. The technical implementation of our new designs employs a Wizard of Oz approach to visually displace Facebook's default privacy authorization dialogues for third-part apps. We use a monitoring infrastructure based on a Google Chrome browser extension. We choose Google Chrome because it has now achieved the highest browser market share (StatCounter 2012). During the study, the Chrome browser extension will be integrated into the authorization process by capturing a particular Facebook app's unique ID. Once the unique ID of that app is captured, the extension either replaces the original privacy authorization dialogue with one of our two proposed redesigns (shown in Figure 2 and Figure 3), or keeps the original interface

(shown in Figure 1). All redesigns are fully functional, i.e., all control boxes are clickable and the tool-tip alert information is available. In all cases, we activate a redirect URL (to a debriefing survey) when participants click the "Allow" and "Don't allow" button. All these replacements are implemented by modifying the privacy authorization page's HTML Document Object Model (DOM). The extension also records users' interaction with the interface and the time they spend on that page. The extension neither records any identifiable information pertaining to Facebook users, nor calls the Facebook API to collect information from users' profiles.

Evaluation: Ongoing Research

Experiment Design

Our research design will use complementary strategies for empirical evaluation, integrated with qualitative and quantitative methods. Interviews will first be conducted to explore users' general privacy attitudes and behaviors and to evaluate our designs. Upon completing the prototype implementation, field experiments will be conducted. We plan to recruit participants via Amazon Mechanical Turk (MTurk). MTurk is often used to obtain high-quality data inexpensively and rapidly, with participants who are more demographically diverse than are standard Internet samples (Buhrmester et al. 2011). On MTurk, requesters post Human Intelligence Tasks (HITs) by uploading job descriptions onto Amazon's web portal. MTurk maintains each Turker's performance history, which requesters may use to specify who is eligible to perform a particular HIT. The requester must also specify the amount of payment a Turker will receive if she completes the task and her work is accepted by the requester.

As Smith et al. (2011) pointed out, different countries have approached privacy issues differently in their social norms and regulatory structures. Thus, in our study, we will restrict eligibility to Turkers with a North American IP address because the technological and regulatory privacy environments in countries in North America are comparatively similar (Smith et al. 2011). Participants with a previous HIT approval rate of 55% or better will be invited to this study. Meanwhile, they will also be required to be active Facebook users and to be familiar with the Google Chrome browser. We will first ask participants to complete an entry background survey followed by opening our study page in a Chrome browser. For participants that do not have the Chrome browser in their computers, we will provide them with the official download link to install the latest version of the Google Chrome browser. We then will randomly assign the participants to one of the three treatment groups (the original interface and two of our proposed redesigns) and ask them to install our Chrome extension. This is followed by redirecting participants to the installation page of a particular third-party application we implement on Facebook. After logging into their own Facebook accounts, participants will be presented with a privacy authorization dialogue associated with their assigned treatment group. Upon pressing the "Allow" or "Don't Allow" button for the app, participants will be automatically redirected to our post-installation questionnaire to evaluate the effectiveness of those three privacy authorization dialogues on users' perceived fairness, trust and risk beliefs.

Measurement

Behavioral Measures

Prior research suggests that there is a strong correlation between eye and mouse movements while users are interacting with the webpage (Pan et al. 2004). To systematically evaluate how our proposed design elements impact users when they interact with the authentication dialog, we will embed an open-source mouse tracking system (smt) (Leiva and Vivó 2007) in our interfaces to collect data on a user's real behaviour. To evaluate the efficacy of the checkbox design elements (i.e., empowering control in Design Principle #1), users' mouse clicks will be captured to observe their interaction patterns with the checkboxes, as well as their app installation decisions. Mouse movement patterns in terms of movement traces and hotspots will be collected to evaluate the efficacy of the layout of permissions and the efficacy of the "i" mark design element (i.e., promoting awareness in Design Principle #2). We will also capture the total amount of time users spend on privacy authentication dialogues.

Scales

The measurement scales used in the post-experimental questionnaire will be adapted from scales used in prior studies. Perceived fairness will be measured by items directly taken from Son and Kim (2008); trust and risk belief will be measured by items taken from Malhotra et al. (2004). Upon collecting the data, we will analyze them using structural equation modelling (SEM) techniques. The statistical techniques selected for SEM will be Partial least squares (PLS). We will use PLS to perform confirmatory factor analysis to assess validity of all multi-item research constructs. The validity of the constructs will be assessed in terms of unidimensionality, convergent validity, internal consistency, and discriminant validity. After establishing the validity of the measures, we will empirically assess the effectiveness of our proposed privacy authorization dialogues on influencing users' perceived fairness, trust and risk beliefs.

Conclusion

As Barkhuus (2012) points out when observing the state-of-the-art in the privacy literature, "it is rare to see studies that implemented real systems with real data sharing or which used in-situ data." To respond to the compelling call for "contextually-grounded research that explores privacy issues in the wild (Barkhuus 2012)," we have designed a field experiment to study users' privacy behaviours mediated through the real system-in-use. Specifically, drawing on the theoretical framework developed by Malhotra et al. (2004), we propose two new designs of privacy authorization dialogues to encompass *control* and *awareness* as the essential factors to address users' privacy concerns pertaining to third-party apps. The approach of *Privacy by ReDesign* is applied to investigate whether users can more adequately represent their preferences for releasing personal information with two improved designs of privacy authorization dialogues. We believe that, building on the groundwork laid down in this study, future research could contribute significantly to minimizing users' privacy concerns in online social networks and, specifically, when using third-party apps. In addition, prior research (e.g., Xu et al. 2011) has identified contextual differences in terms of individuals' privacy attitudes and perceptions in different domains such as e-commerce, social media, finance, and healthcare. Therefore, another implication for future research is to extend and adapt the approach described in this work to other domains that raise similar or more complex privacy issues.

Acknowledgements

The authors are grateful to the associate editor and reviewers for their constructive comments on the earlier version of this manuscript. Heng Xu gratefully acknowledges the financial support of the U.S. National Science Foundation under grant CNS-0953749. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. National Science Foundation.

References

Acquisti, A., and Gross, R. 2009. "Predicting Social Security Numbers from Public Data," *Proceedings of the National Academy of Sciences* (106:27), pp 10975-10980.

Barkhuus, L. 2012. "The Mismeasurement of Privacy: Using Contextual Integrity to Reconsider Privacy in Hci," *Proceedings of the ACM Annual Conference on Human Factors in Computing Systems*, Austin, Texas, USA: ACM, pp. 367–376.

Besmer, A., and Lipford, H. 2010. "Users' (Mis)Conceptions of Social Applications," *Proceedings of Graphics Interface (GI'10)*, Ottawa, Canada: Canadian Information Processing Society, pp. 63-70.

Buhrmester, M., Kwang, T., and Gosling, S.D. 2011. "Amazon's Mechanical Turk a New Source of Inexpensive, yet High-Quality, Data?," *Perspectives on Psychological Science* (6:1), pp 3-5.

Cavoukian, A., and Prosch, M. 2011. "Privacy by Redesign: Building a Better Legacy." from http://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1070

Colquitt, J., A., Conlon, D.E., Wesson, M.J., Porter, C., and Ng, K.Y. 2001. "Justice at the Millenium: A Meta-Analytic Review of 25 Years of Organisational Justice Research," *Journal of Applied Psychology* (86:3), pp 425-445.

Gregor, S., and Jones, D. 2007. "The Anatomy of a Design Theory," *Journal of the Association for Information Systems* (8:5), pp 312-335.

Gross, R., and Acquisti, A. 2005. "Information Revelation and Privacy in Online Social Networks," in: *Proceedings of the ACM Workshop on Privacy in the Electronic Society*. Alexandria, VA, USA.

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. "Design Science in Information Systems Research," *MIS Quarterly* (28:1), pp 75-105.

Hoadley, C.M., Xu, H., Lee, J.J., and Rosson, M.B. 2010. "Privacy as Information Access and Illusory Control: The Case of the Facebook News Feed Privacy Outcry," *Electronic Commerce Research and Applications* (9:1), pp 50-60.

Hoffman, D.L., Novak, T.P., and Peralta, M.A. 1999. "Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web," *Information Society* (15:2), pp 129-139.

Jagatic, T.N., Johnson, N.A., Jakobsson, M., and Menczer, F. 2007. "Social Phishing," *Communications of the ACM* (50:10), pp 94-100.

KCG. 2006. "Evolution of a Prototype Financial Privacy Notice." *Kleimann Communication Group, Inc.*, from http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf

Kelley, G.P., Bresee, J., Cranor, F.L., and Reeder, W.R. 2009. "A Nutrition Label for Privacy," in: *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View, California, USA: ACM, pp. 1-12.

Leiva, L.A., and Vivó, R. 2007. "(Smt) Real Time Mouse Tracking Registration and Visualization Tool for Usability Evaluation on Websites," *Proceedings of IADIS WWW/Internet*, Vila Real, Portugal, pp. 187-192.

Malhotra, N.K., Kim, S.S., and Agarwal, J. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* (15:4), pp 336-355.

Pan, B., Hembrooke, H.A., Gay, G.K., Granka, L.A., Feusner, M.K., and Newman, J.K. 2004. "The Determinants of Web Page Viewing Behavior: An Eye-Tracking Study," *Proceedings of the Symposium on Eye Tracking Research & Applications*, San Antonio, Texas, USA: ACM, pp. 147-154.

Phelps, J., Nowak, G., and Ferrell, E. 2000. "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy and Marketing* (19:1), pp 27-41.

Sein, M., Henfridsson, O., Purao, S., Rossi, M., and Lindgren, R. 2011. "Action Design Research," *MIS Quarterly* (35:1), pp 37-56.

Sheehan, K.B., and Hoy, M.G. 2000. "Dimensions of Privacy Concern among Online Consumers," *Journal of Public Policy & Marketing* (19:1), pp 62-73.

Smith, H.J., Dinev, T., and Xu, H. 2011. "Information Privacy Research: An Interdisciplinary Review," *MIS Quarterly* (35:4), pp 989-1015.

Smith, H.J., Milberg, J.S., and Burke, J.S. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices," *MIS Quarterly* (20:2), June, pp 167-196.

Solove, D.J. 2006. "A Taxonomy of Privacy," *University of Pennsylvania Law Review* (154:3), pp 477-560.

Son, J.-Y., and Kim, S.S. 2008. "Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model," *MIS Quarterly* (32:3), pp 503-529.

StatCounter. 2012. "Statcounter Global Stats." Retrieved Sept 8, 2012, from http://gs.statcounter.com/

Steel, E., and Fowler, G. 2010. "Facebook in Privacy Breach," *The Wall Street Journal*, October 18th.

Stewart, K.A., and Segars, A.H. 2002. "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp 36-49.

Wang, N., Xu, H., and Grossklags, J. 2011. "Third-Party Apps on Facebook: Privacy and the Illusion of Control," *Proceedings of the ACM Symposium on Computer-Human Interaction for Management of Information Technology (CHIMIT)*, Boston, MA, USA: ACM, pp. 1-10.

Xu, H., Dinev, T., Smith, H.J., and Hart, P. 2011. "Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances," *Journal of the Association for Information Systems* (12:12), pp 798-824.